Claims

What is claimed is:

1. A method for performing a computational task associated with a cryptographic protocol in a distributed manner using a plurality of machines, the plurality of machines comprising an originator machine and at least one additional machine, the method comprising the steps of:

transforming a computational task involving a given input in the originator machine, the transforming of the computational task involving at least an error-related operation, a blinding operation and a permutation operation;

sending the transformed computational task to the at least one additional machine for execution;

receiving one or more results of the transformed computational task in the originator machine; and

transforming the one or more results of the transformed computational task in the originator machine in a manner which permits verification that the one or more results are appropriate results for the given input.

2. The method of claim 1 wherein the operation associated with the cryptographic protocol comprises an exponentiation operation.

3. The method of claim 1 wherein the cryptographic protocol comprises a digital signature protocol.

4. The method of claim 1 wherein at least a subset of the originator machine and the at least one additional machine each comprise one or more servers associated with a computer network.

5. The method of claim 1 wherein the originator machine and the at least one additional machine communicate over a network.

6. The method of claim 1 wherein the originator machine includes a card reader configured to read information relating to the cryptographic protocol from a smart card.

7. The method of claim 1 wherein the blinding operation is applied to an output of the error-related operation, and the permutation operation is applied to an output of the blinding operation.

8. The method of claim 1 wherein the error-related operation comprises a replication operation and a dependency operation.

9. The method of claim 8 wherein the dependency operation is applied to an output of the replication operation.

10. The method of claim 1 wherein the computational task to be transformed is a request to compute $\left(g^{k_1},\ldots,g^{k_n}\right)$ denoted by a vector $G_1 = (k_1, . . . , k_n)$ where g denotes a generator and k_1, . . . , k_n denote portions of a secret key associated with the cryptographic protocol.

11. The method of claim 1 wherein the error-related operation includes one or more replication operations.

12. The method of claim 1 wherein the error-related operation includes a replication operation in which a first vector $G_1 = (k_1, . . . , k_n)$ is transformed into a second vector

$$G_2 = (k_1, . . . k_n, k_{n+1}, k_1, . . . , . . . , k_n, k_{n+1}, k_1, . . . , k_n, k_{n+1}).$$

13. The method of claim 1 wherein the error-related operation includes a dependency operation in which dependencies are introduced between two or more computational tasks.

14. The method of claim 1 wherein the error-related operation includes a dependency operation in which dependencies are introduced transforming a computational task involving a set of exponents $k_1, \ldots, k_n$ into a task involving the exponents $k_1', \ldots, k_n'$, where

$$k_i' = \begin{cases} k_1 & : \ i = 1 \\ k_i + \alpha \cdot k_{i-1} + \beta \cdot k_{i-1}' \bmod q & : \ 1 < i \leq n \end{cases}.$$

15. The method of claim 1 wherein the blinding operation blinding for a vector $(k_1, \ldots, k_n)$ is implemented by first choosing e random numbers $r_1, \ldots r_e \in \{0, \ldots, \frac{q-1}{2}\}$, and then, for each element k_j with $1 \leq j \leq n$, d elements are chosen and elements of a new vector are computed as

$$k_j' = k_j - \sum_{i=1}^{e} \gamma_{i,j} r_i \bmod q$$

where $\gamma_{i,j} \in \{0, 1\}$ and $\sum_{i=1}^{e} \gamma_{i,j} = d$.

16. The method of claim 1 wherein the permutation operation comprises applying a permutation Π selected uniformly at random to a vector output of the blinding step to generate a new vector corresponding to the transformed computational task.

17. The method of claim 1 wherein the results of the transformed computation are transformed by inversion of the permutation operation followed by inversion of the blinding operation, and the transformed results are verified based on information associated with the error-related operation.

18. An apparatus for performing a computational task associated with a cryptographic protocol in a distributed manner using a plurality of machines, the plurality of machines comprising an originator machine and at least one additional machine, the apparatus comprising:

a processor associated with the originator machine and operative to transform a computational task involving a given input in the originator machine, the transforming of the computational task involving at least an error-related operation, a blinding operation and a permutation operation, to send the transformed computational task to the at least one additional machine for execution, to receive one or more results of the transformed computational task, and to transform the one or more results of the transformed computational task in a manner which permits verification that the one or more results are appropriate results for the given input; and

a memory coupled to the processor for at least temporarily storing at least a portion of the results of the transformed computational task.

19. A computer-readable medium containing one or more programs for performing a computational task associated with a cryptographic protocol in a distributed manner using a plurality of machines, the plurality of machines comprising an originator machine and at least one additional machine, wherein the one or more programs when executed in a processor provide the steps of:

transforming a computational task involving a given input in the originator machine, the transforming of the computational task involving at least an error-related operation, a blinding operation and a permutation operation;

sending the transformed computational task to the at least one additional machine for execution;

receiving one or more results of the transformed computational task in the originator machine; and

transforming the one or more results of the transformed computational task in the originator machine in a manner which permits verification that the one or more results are appropriate results for the given input.